Docket: T2146-907683-US 3879/BC

IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (D.O./E.O./US)

Applicant:	Michel HAZARD
International Application No.:	PCT/FR01/01359
International Filing Date:	4 May 2001
U.S. Serial No.:	To be assigned
U.S. Filing Date:	January 9, 2002
For:	**METHOD FOR AUTHENTICATING A PORTABLE OBJECT, CORRESPONDING PORTABLE OBJECT, AND APPARATUS THEREFOR**

McLean, Virginia

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

The following amendments and remarks are submitted prior to examination of the above-identified application on the merits.

IN THE SPECIFICATION

After the title and before the first paragraph **[0001]**, insert the following:

--BACKGROUND OF THE INVENTION

1. Field of the Invention.

This invention relates to product security, and more particularly to a system and method for verifying the authenticity of a product or service in connection with a personal, business, or commercial transaction.

2. Description of the Related Art.--

Page 1, before paragraph **[0004]** insert the following header:

--SUMMARY OF THE INVENTION--;

Page 3, before paragraph **[0009]**, insert the following header:

--BRIEF DESCRIPTION OF THE DRAWINGS--;

Page 3, before paragraph **[0010]**, insert the following header:

--DESCRIPTION OF THE PREFERRED EMBODIMENTS--;

Page 11, end of page, insert a new paragraph **[0040]:**

--**[0040]** While this invention has been described in conjunction with specific embodiments thereof, it is evident that many alternatives, modifications and variations will be apparent to those skilled in the art. Accordingly, the preferred embodiments of the invention as set forth herein, are intended to be illustrative, not limiting. Various changes may be made without departing from the true spirit and full scope of the invention as set forth herein and defined in the claims.—

Page 12, after the last line, insert the following:

--I claim:--

IN THE CLAIMS

Please substitute amended claims 1-15 as presented below for the same-numbered claims that were pending prior to the filing of this paper. A marked-up version of the amended claims is attached.

1. (Amended) A method for authenticating a portable object including information processing means and information storage means, the information storage means containing at least one code defining operation steps capable of being executed by the portable object, as well as a one-way function, comprising sending the portable object an order for executing a calculation of a result by applying to said one-way function at least part of said code and using said result to decide whether or not the portable object is authentic.

2. (Amended) A method according to claim 1, wherein said result enters into the implementation of a predetermined operation, said operation being performed successfully only when the portable object is authentic.

3. (Amended) A method according to claim 2, wherein said predetermined operation comprises a decryption operation, said result making it possible to produce an associated decryption key.

4. (Amended) A method according to claim 1, wherein said part of said code used in the calculation, comprises a machine code.

5. (Amended) A method according to claim 1, wherein the portable object contains a real code defining operations designed to be executed by the portable object, and a dummy code defining operations not designed to be executed by the portable object, said code used in the calculation of a result comprising a dummy code.

6. (Amended) A method according to claim 1, further comprising repeatedly sending said order to the portable object during its life, prior to execution by the portable object of said operation steps.

7. (Amended) A method according to claim 1, wherein said code used in the calculation is defined by a start address and an end address in the information storage means, and further including the step of sending said start and end addresses to the portable object.

8. (Amended) A method according to claim 1, wherein said code comprises a set of binary words, said code used in the calculation being defined by a subset of said binary words comprising binary words distributed in the information storage means at a determined pitch, said pitch being sent to the portable object.

9. (Amended) A method for having a portable object execute a sensitive operation, the portable object comprising information processing means and information storage means, comprising: storing in the information storage means at least one code defining operations capable of being executed by the portable object, as well as a one-way function, and sending the portable object an order so that the portable object executes a calculation of a result by applying to said one-way function at least part of said code, said result entering into the implementation of said sensitive operation, said operation being performed successfully only when the portable object is authentic.

10. (Amended) A method according to claim 9, wherein the code part used in the calculation comprises a machine code.

11. (Amended) A method according to claim 9, wherein the portable object contains a real code defining operations designed to be executed by the portable object, and a dummy code defining operations not designed to be executed by the portable object, said code part used in the calculation comprising a dummy code.

12. (Amended) A portable object, comprising: information processing means, information storage means, the information storage means containing at least one code defining operations capable of being executed by the portable object, as well as a one-way function, and means for executing a calculation of a result by applying to said one-way function at least part of said code.

13. (Amended) A portable object according to claim 12, wherein said code part used in the calculation comprises a machine code.

14. (Amended) A device comprising: information processing means, information storage means, said information processing means designed to communicate with a portable object in order to authenticate the portable object, the portable object comprising: information processing means, information storage means, the information storage means of the portable object containing at least one code defining operations capable of being executed by the portable object, as well as a one-way function, and means for sending the portable object an order so that

the portable object executes a calculation of a result by applying to said one-way function at least part of said code of the portable object.

15. (Amended) A device according to claim 14, wherein said code part used in the calculation comprises a machine code.

IN THE ABSTRACT

Please replace the Abstract as originally filed with the following new abstract:

--ABSTRACT

A method for authenticating a portable object includes an information processing means and an information storage means. The information storage means contains at least one code defining operations capable of being executed by the portable object, as well as a one-way function. The method comprises sending the portable object an order so that the latter executes a calculation of a result by applying to said one way function at least part of said code. This result is used to decide whether or not the portable object is authentic.--

REMARKS

Claims 1-15 are pending. These claims have been amended to place them in a form which comports with established U.S. claim practice. Also, the specification has been amended to include section headers, and a new abstract has been provided.

It is respectfully submitted that the application is in condition for allowance. Favorable consideration and prompt allowance of the application is respectfully requested.

Should the Examiner believe that further amendments are necessary to place the application in condition for allowance, or if the Examiner believes that a personal interview would be advantageous in order to more expeditiously resolve any remaining issues, the Examiner is invited to contact Applicant's undersigned attorney at the telephone number listed below.

To the extent necessary, Applicant petitions for an extension of time under 37 CFR § 1.136. Please charge any shortage in fees due in connection with this application, including extension of time fees, to Deposit Account No. 50-1165 (Attorney Docket No. T2146-907683) and credit any excess fees to the same Deposit Account.

Respectfully submitted,

Miles & Stockbridge P.C.

Date: January 9, 2002

By: Edward J. Kondracki
Edward J. Kondracki
Registration No. 20,604

1751 Pinnacle Drive, Suite 500
McLean, Virginia 22102-3833
Telephone No: (703) 610-8641
Facsimile No: (703) 610-8686

Marked-Up Version of the Amended Claims

1. (Amended) [Method] A method for authenticating a portable object [(7) comprising] including information processing means [(8)] and information storage means [(9, 10)], the information storage means containing at least one code [(i)] defining [operations] operation steps capable of being executed by the portable object, as well as a one-way function, [characterized in that it comprises the step that consists of] comprising sending the portable object an order [(31, 32i-34i, 35, 36) so that the latter executes a] for executing a calculation of a result by applying to said one-way function at least part of said code [(i)], [this] and using said result [being used] to decide whether or not the portable object is authentic.

2. (Amended) [Method] A method according to claim 1, wherein said result enters into the implementation of a [given] predetermined operation, [this] said operation being performed successfully only when the portable object [(7)] is authentic.

3. (Amended) [Method] A method according to claim 2, wherein said [given] predetermined operation comprises a decryption operation, said result making it possible to produce an associated decryption key.

4. (Amended) [Method] A method according to claim 1, wherein said part of said code [part (i)] used in the calculation, comprises a machine code [part].

5. (Amended) [Method] A method according to claim 1, wherein the portable object [(7)] contains a [so-called "real"] real code defining operations designed to be executed by the portable object, and a [so-called "dummy"] dummy code defining operations not designed to be executed by the portable object, said code [part] used in the calculation of a result comprising a dummy code [part].

6. (Amended) [Method] A method according to claim 1, [wherein said order (31, 32i-34i, 35, 36) is sent] further comprising repeatedly sending said order to the portable object [repeatedly] during its life, prior to [the] execution by the [latter] portable object of said [operations] operation steps.

7. (Amended) [Method] A method according to claim 1, wherein said code [part (i)] used in the calculation is defined by a start address [(32i)] and an end address [(33i)] in the information storage means, and further including the step of sending said start and end addresses [being sent] to the portable object.

8. (Amended) [Method] A method according to claim 1, wherein said code [(i)] comprises a set of binary words, said code [part] used in the calculation being defined by a subset of said binary words comprising [the] binary words distributed in the information storage means at a determined pitch [(34i)], said pitch being sent to the portable object.

9. (Amended) [Method] A method for having a portable object [(7)] execute a sensitive operation, the portable object comprising information processing means [(8)] and information storage means [(9, 10)], comprising: storing in the

information storage means [containing] at least one code [(i)] defining operations capable of being executed by the portable object, as well as a one-way function, and [characterized in that it comprises the step that consists of] sending the portable object an order [(31, 32i-34i, 35, 36)] so that the [latter] portable object executes a calculation of a result by applying to said one-way function at least part of said code [(i)], said result entering into the implementation of said sensitive operation, [this] said operation being performed successfully only when the portable object [(7)] is authentic.

10. (Amended) [Method] A method according to claim 9, wherein [said] the code part [(i)] used in the calculation comprises a machine code [part].

11. (Amended) [Method] A method according to claim 9, wherein the portable object contains a [so-called "reel"] real code defining operations designed to be executed by the portable object, and a [so-called "dummy"] dummy code defining operations not designed to be executed by the portable object, said code part used in the calculation comprising a dummy code [part].

12. (Amended) [Portable] A portable object, comprising: information processing means, [(8) and] information storage means [(9, 10)], the information storage means containing at least one code [(i)] defining operations capable of being executed by the portable object, as well as a one-way function, [characterized in that it comprises] and means for executing a calculation of a result by applying to said one-way function at least part of said code.

13. (Amended) [Portable] A portable object according to claim 12, wherein said code part [(i)] used in the calculation comprises a machine code [part].

14. (Amended) [Device (1)] A device comprising: information processing means, [(2) and] information storage means [(3, 4) and] , said information processing means designed to communicate with a portable object [(7)] in order to authenticate the [latter] portable object, the portable object comprising: information processing means, [(8) and] information storage means [(9, 10)], the information storage means of the portable object containing at least one code [(i)] defining operations capable of being executed by the portable object, as well as a one-way function, [characterized in that it comprises] and means for sending the portable object an order [(31, 32i-34i, 35, 36)] so that the [latter] portable object executes a calculation of a result by applying to said one-way function at least part of said code [(i)] of the portable object.

15. (Amended) [Device] A device according to claim 14, wherein said code part [(i)] used in the calculation comprises a machine code [part].

T2146-907683-US 3879/BC

IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (D.O./E.O./US)

Applicant:	Michel HAZARD
International Application No.:	PCT/FR01/01359
International Filing Date:	4 May 2001
U.S. Serial No.:	To be assigned
U.S. Filing Date:	January 9, 2002
For:	**METHOD FOR AUTHENTICATING A PORTABLE OBJECT, CORRESPONDING PORTABLE OBJECT, AND APPARATUS THEREFOR**

McLean, Virginia

PROPOSED DRAWING CORRECTIONS

Hon. Commissioner of Patents and Trademarks
Washington, D.C. 20231

Sir:

Applicant requests approval of the drawing corrections on Figs. 1 – 4 as shown in red on the attached two (2) sheets.

The proposed corrections only comprise translation of the French terms in the blocks to correspond the drawings to the specification and claims and removing the headings "1/2" and "2/2" to correspond the drawings to U.S. practice..

Respectfully submitted,

Miles & Stockbridge P.C.

Date: January 9, 2002

By: Edward J. Kondracki
Registration No. 20,604

1751 Pinnacle Drive, Suite 500
McLean, Virginia 22102-3833
Telephone No: (703) 610-8641
Facsimile No: (703) 610-8686